DoD Spear-Phishing Awareness Training

Joint Task Force - Global Network Operations

Updated: 16 NOV 2006

Objective

- **Inform and increase the awareness of all Department of Defense personnel of the dangers and threats imposed on DoD information systems as a result of "spear-phishing" emails.**

- **Instruct personnel on how to recognize these email threats while offering methods to help counter the threat.**

Instructions

- To advance to the next slide, click the button

- Click to return to the previous slide.

- Click on the hyperlinked (blue, underlined) text to get more information on an item.

What is “Phishing”?

Phishing is a criminal activity using social engineering techniques.

“Phishers” attempt to fraudulently acquire sensitive information, such as passwords, personal information, military operations, and credit card/financial details, by masquerading as a trustworthy person or business in an electronic communication.

BUT…DID YOU KNOW……

Hidden Threats of "Phishing"

Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software.

What this means…

These emails may contain mini-programs that will be installed on your computer.

They may capture your keystrokes or capture your personal files and send them to people they shouldn't be going

Hidden Threats of "Phishing"

Most phishing attempts are for identity theft, but there is a rise in attempts at gaining access to online banking, federal, and defense information.

These hidden/unknown threats can capture your passwords/login credentials and also compromise unclassified, but yet sensitive, information that can put Department of Defense operations at

What is “Spear Phishing”?

Spear Phishing is a GREATER threat!!!

Spear Phishing is a highly targeted phishing attempt.

The attacker selectively chooses the recipient (target) and usually has a thorough understanding of the target’s command or organization.

What is “Spear Phishing”?

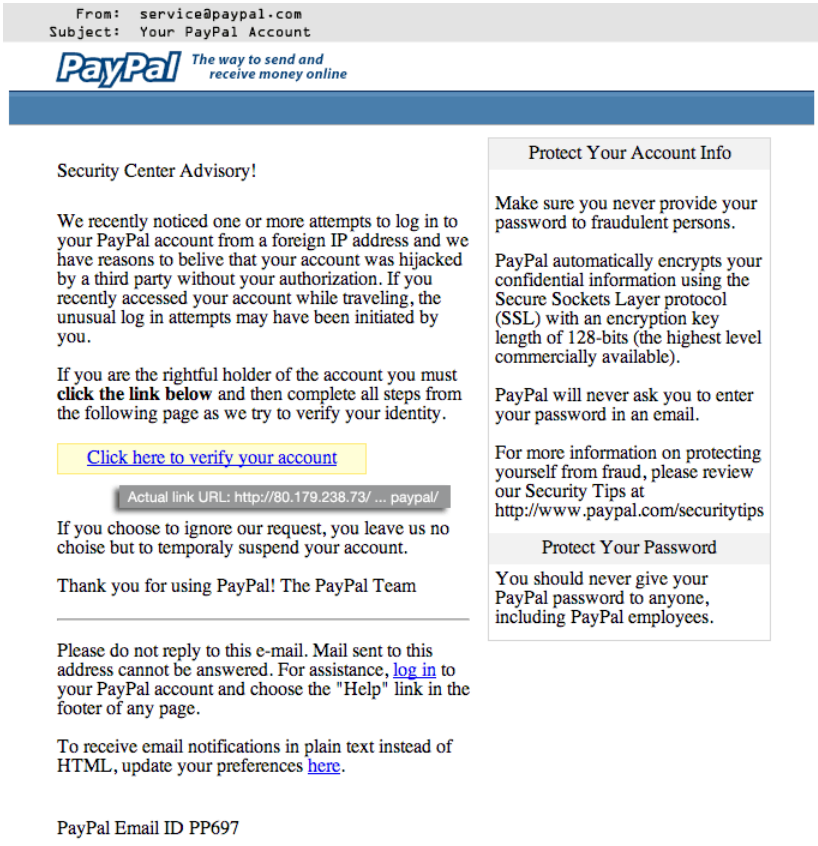
The attacker may:

- **Address the recipient by name**
- **Use lingo/jargon of the organization**
- **Reference actual procedures, SOPs/TTPs, or DOD Instructions**

The email may appear very genuine. Sometime these emails have legitimate operational and exercise nicknames, terms, and key words in the subject and body of the message.

Common Examples of Phishing

Phishing is not anything new and many of you may have seen examples in emails from your personal / at-home accounts.



From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

- **You may have seen emails that appear to come from your bank or other online financial institutions.**

Commonly Seen Commercial Examples:

eBay, PayPal, all banking and financial institutions

Bank of America Military Bank

Phishing Email sent portraying Bank of America, Military Bank

Entices the user to complete a survey and

Dear Customer,
Bank of America Military Bank is doing a 20$ Reward Survey. Bank of America Military Bank will add $20 credit to your account just for taking part in our quick 5 easy question survey. To get advantage of this offer click on the link below.

< URL REMOVED >

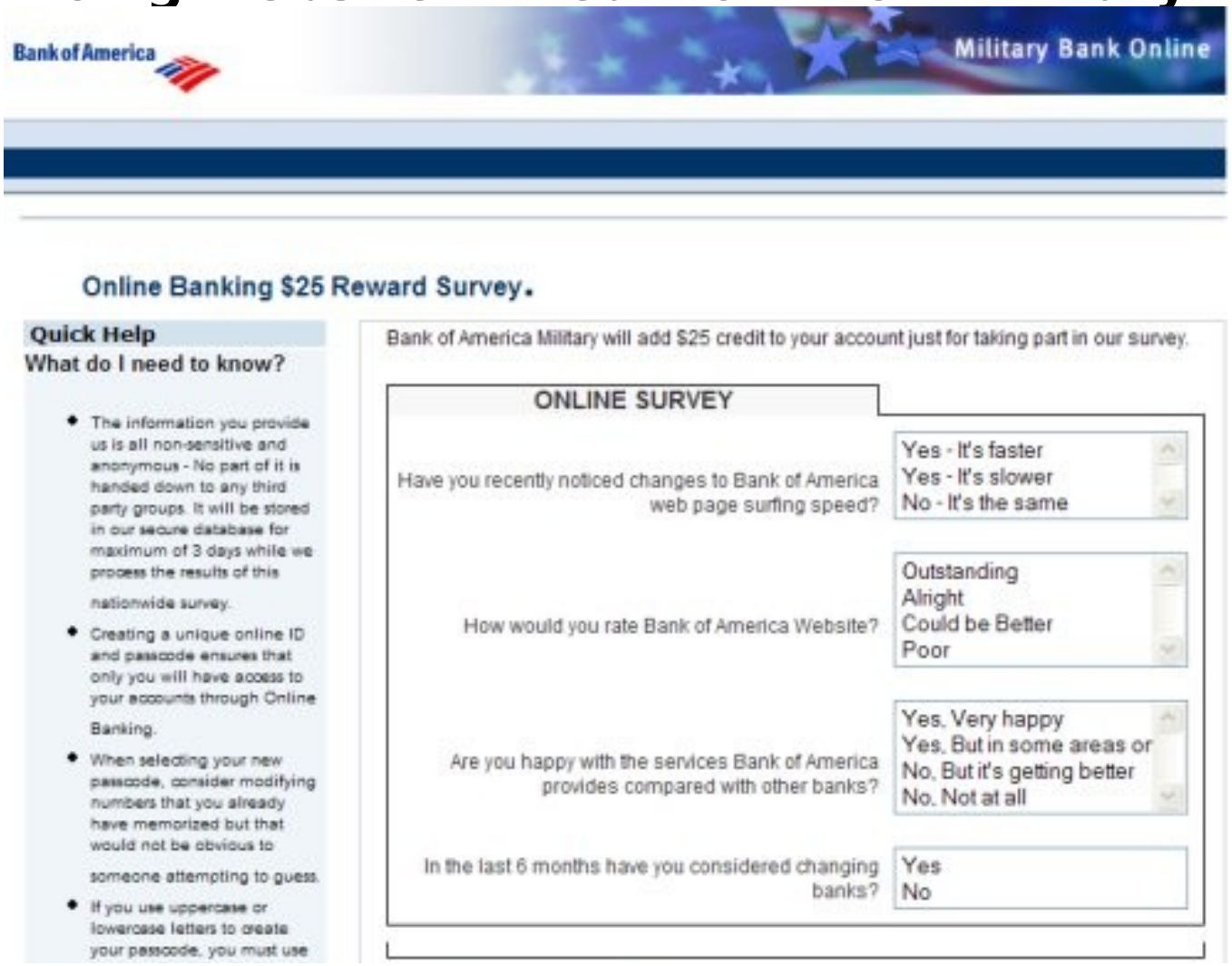
This message has been sent only to our special customers.

Thank you,

Bank of America Military Bank Customer Service

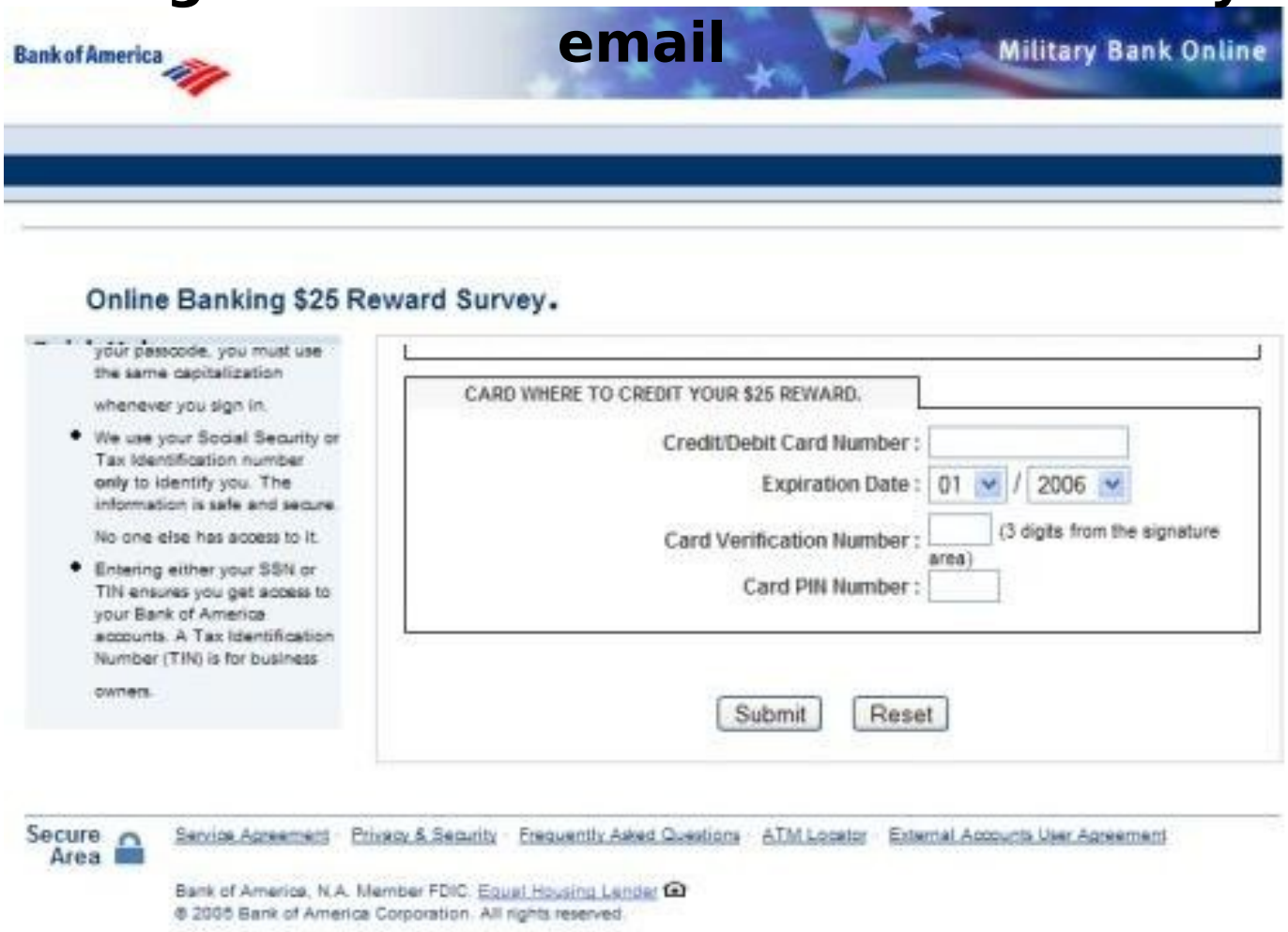
Bank of America Military Bank

Convincing website linked from BOA Military Bank


Bank of America
Military Bank Online
Online Banking $25 Reward Survey.
Quick Help
What do I need to know?
The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups. It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey.
Creating a unique online ID and passcode ensures that only you will have access to your accounts through Online Banking.
When selecting your new passcode, consider modifying numbers that you already have memorized but that would not be obvious to someone attempting to guess.
If you use uppercase or lowercase letters to create your passcode, you must use
Bank of America Military will add $25 credit to your account just for taking part in our survey.
ONLINE SURVEY
Have you recently noticed changes to Bank of America web page surfing speed?
Yes - It's faster
Yes - It's slower
No - It's the same
How would you rate Bank of America Website?
Outstanding
Alright
Could be Better
Poor
Are you happy with the services Bank of America provides compared with other banks?
Yes, Very happy
Yes, But in some areas or
No, But it's getting better
No, Not at all
In the last 6 months have you considered changing banks?
Yes
No

Bank of America Military Bank

Convincing website linked from BOA Military Bank email


Bank of America
Military Bank Online
Online Banking $25 Reward Survey.
your passcode, you must use the same capitalization whenever you sign in.
We use your Social Security or Tax Identification number only to identify you. The information is safe and secure. No one else has access to it.
Entering either your SSN or TIN ensures you get access to your Bank of America accounts. A Tax Identification Number (TIN) is for business owners.
CARD WHERE TO CREDIT YOUR $25 REWARD.
Credit/Debit Card Number :
Expiration Date : 01 / 2006
Card Verification Number : (3 digits from the signature area)
Card PIN Number :
Submit
Reset
Secure Area
Service Agreement
Privacy & Security
Frequently Asked Questions
ATM Locator
External Accounts User Agreement
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2005 Bank of America Corporation. All rights reserved

Should I be worried?

YES, this is occurring within DOD

The attacker's primary focus is to get you to open an attachment or follow a web link. These actions may install the malicious software.

Most spear phishing attacks within DOD are not for identity theft.

Who should be worried?

Everyone within DOD is a target.
Attempts have been seen at all levels and areas.

Military, Civilians, Contractors
All Ranks
All Services
All Geographic Locations

Discovered “spear phishing” messages within the DOD can be *very* convincing

Recognition

- **"From" field of an email can be easily faked (spoofed).**
  - **It might appear completely correct, or have a similar variation.**
    account_security@mypay.com

- **On the other hand, the message may come from a**
  - **legitimate email account, because that account has been compromised.**
    john.smith.yourboss@yourbase.mil

This can occur when the attackers obtain someone's login credentials and email contacts in their address book in order to obtain more accounts.

Recognition

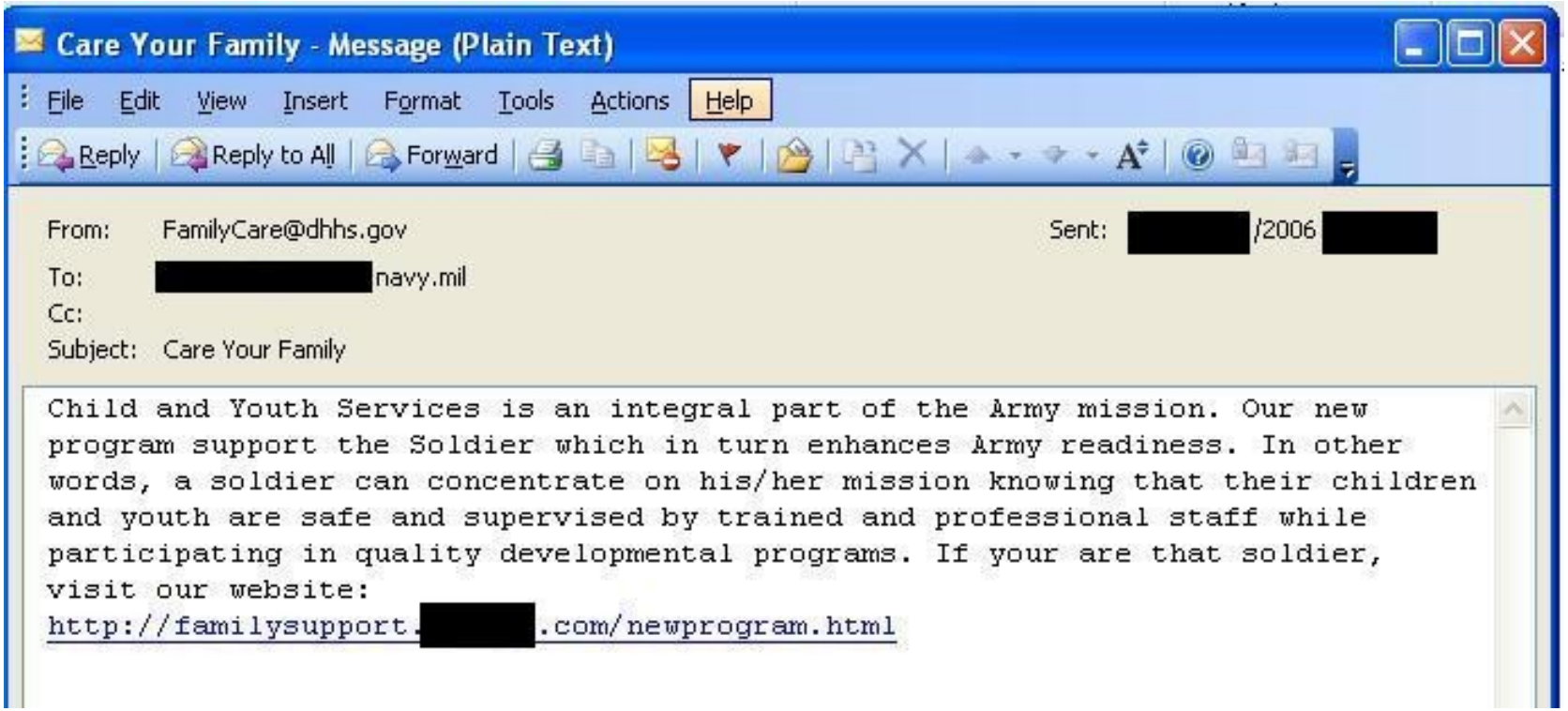
Other recognition factors of phishing attempts:

1) **Generic Greeting**
2) **Fake Sender's Address**
3) **False Sense of Urgency**
4) **Fake Web Links. Deceptive Web Links. Email is requiring that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment.**
5) **Emails that appear like a website**

Recognition (Example 1)

Sanitized example of a message with a link to a website that installs malicious software.

DO NOT FOLLOW THESE LINKS

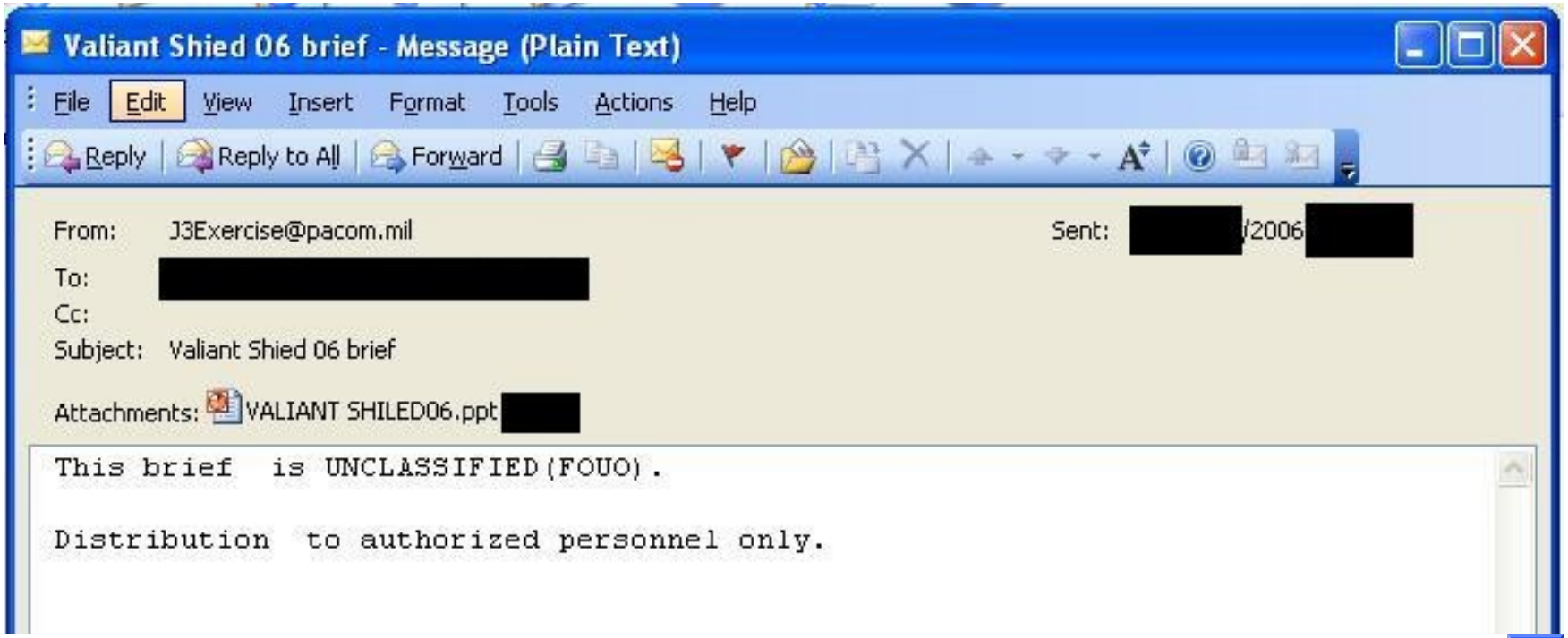

Care Your Family - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: FamilyCare@dhhs.gov
Sent: [redacted]/2006 [redacted]
To: [redacted]navy.mil
Cc:
Subject: Care Your Family
Child and Youth Services is an integral part of the Army mission. Our new program support the Soldier which in turn enhances Army readiness. In other words, a soldier can concentrate on his/her mission knowing that their children and youth are safe and supervised by trained and professional staff while participating in quality developmental programs. If your are that soldier, visit our website:
http://familysupport.[redacted].com/newprogram.html

Recognition (Example 2)

Sanitized example of a message with an attachment that contained malware.

DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL

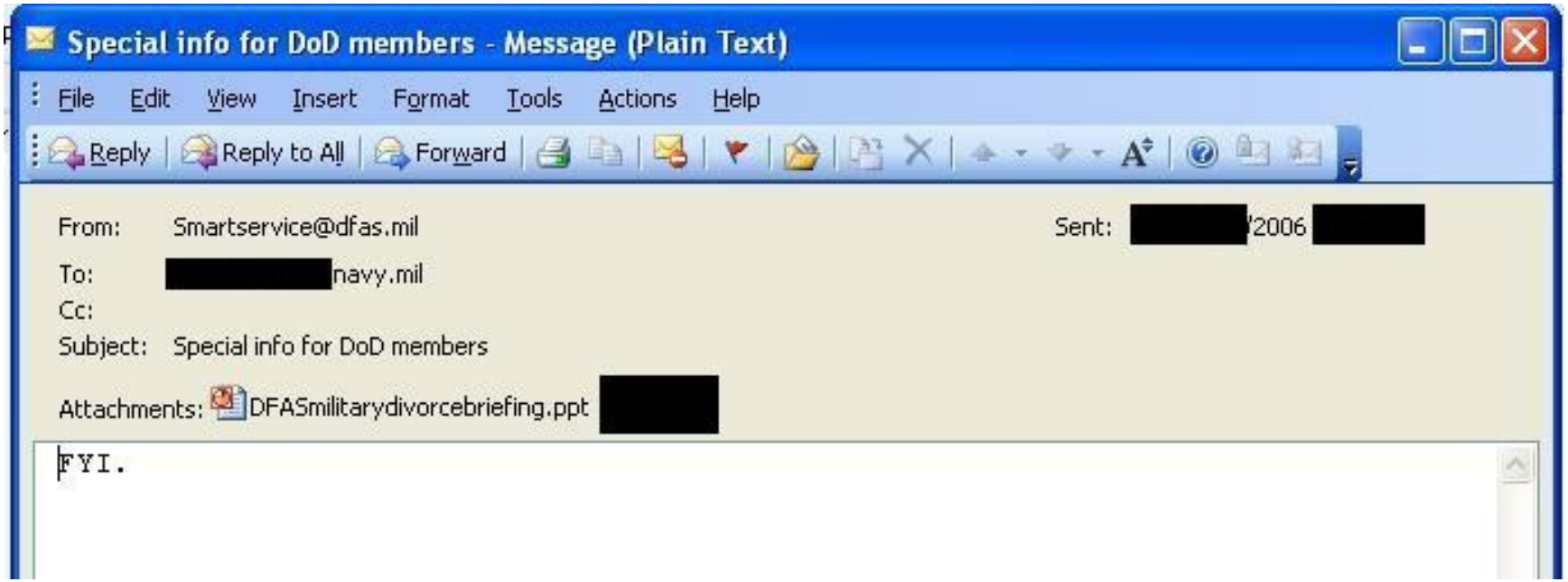
NOTE: VALIANT SHIELD was an actual exercise event. Message was sent from a supposed exercise account.


Valiant Shied 06 brief - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: J3Exercise@pacom.mil
Sent: [redacted]/2006
To: [redacted]
Cc:
Subject: Valiant Shied 06 brief
Attachments: VALIANT SHILED06.ppt [redacted]
This brief is UNCLASSIFIED(FOUO).
Distribution to authorized personnel only.

Recognition (Example 3)

Sanitized example of a message with an attachment that contained malware.

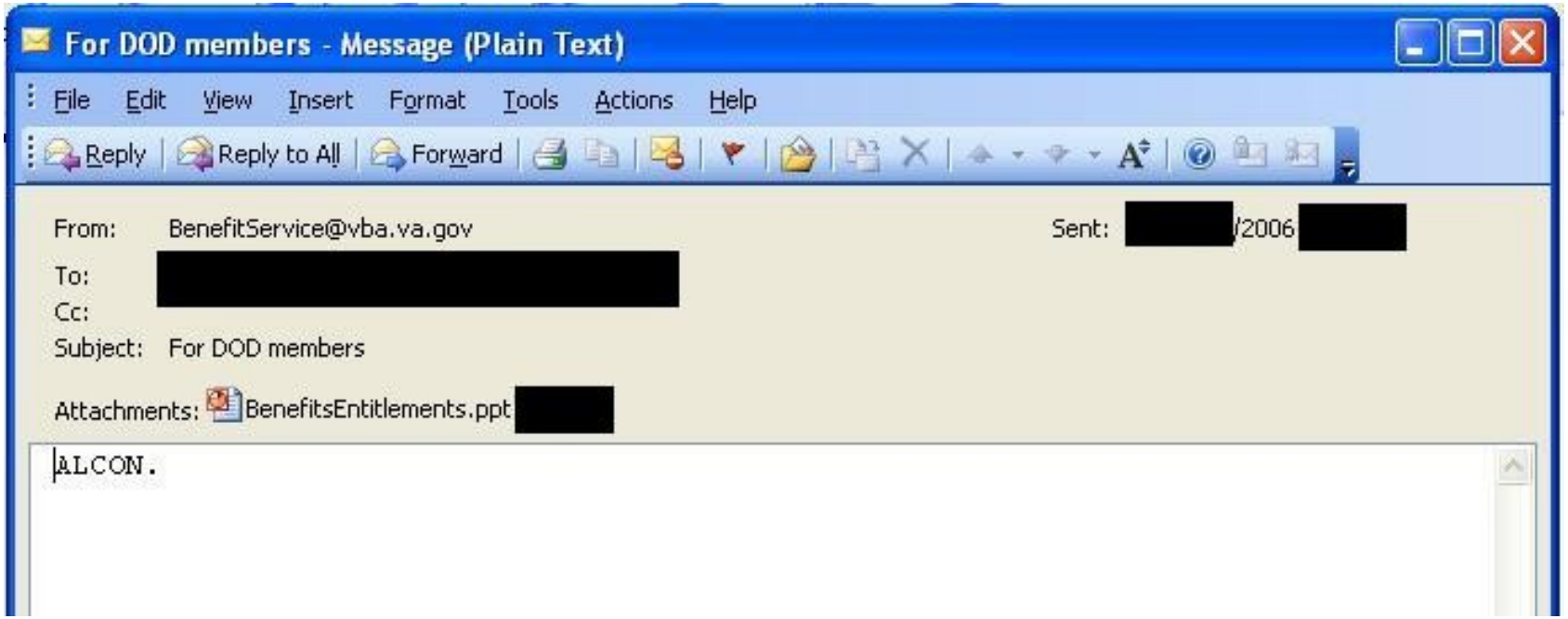
DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL


Special info for DoD members - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: Smartservice@dfas.mil
Sent: [redacted]/2006 [redacted]
To: [redacted]navy.mil
Cc:
Subject: Special info for DoD members
Attachments: DFASmilitarydivorcebriefing.ppt [redacted]
FYI.

Recognition (Example 4)

Sanitized example of a message with an attachment that contained malware.

DO NOT OPEN THE ATTACHMENT IF YOU RECEIVE A SIMILARLY COMPOSED EMAIL



Prevention (as a receiver)

Be cognizant and vigilant of this threat.

Before clicking on any weblink within a message or opening up an attachment, be sure the source of the email is legitimate.

Is it digitally signed?

The links and attachments can contain malware, spyware, viruses, and trojan horses.

If you click on these illegitimate links ents

Prevention (as a sender)

At a minimum,
Digitally Sign All E-mails?

If your position involves official direct email contact with outside DoD entities,
digital signatures might not be an option.

If this is the case, be suspect of the format and enclosed attachments with these individuals.

Prevention (as a sender)

Note on Operations Security (OPSEC)

Users should digitally sign and encrypt all messages that contain: (at a minimum)

- **For Official Use Only (FOUO)**
- **Privacy Act / personal information**
- **technical and contract data**
- **proprietary information**
- **foreign government information**
- **financial information**
- **source selection information**

Prevention (as a sender)

Do not send emails using "*HTML*" formatting.

Use "*Plain Text*" or "*Rich Text*" formatted emails.

"*Plain Text*" (or ASCII) is preferred because Rich Text looks the same as HTML formatting.

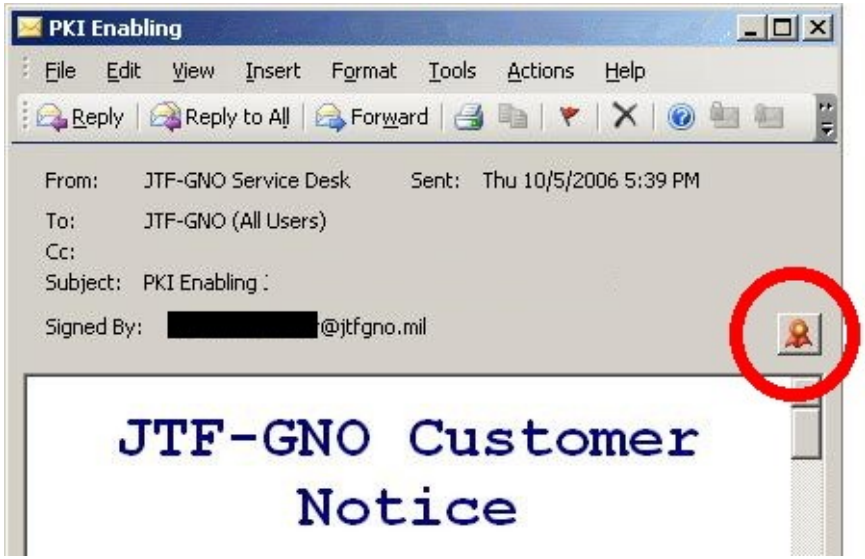
How do I set this up?

Digital Signing

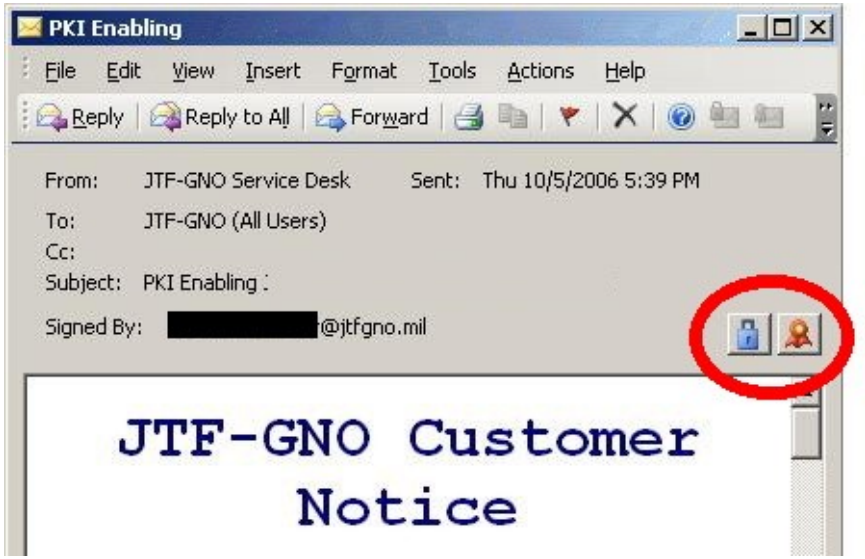
The importance of digitally signing your messages can't be stressed enough.

To date, there are no known "spoofs" to digital signatures, other than compromised PKI credentials due to negligence.

Digitally Signed Message


PKI Enabling
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: JTF-GNO Service Desk Sent: Thu 10/5/2006 5:39 PM
To: JTF-GNO (All Users)
Cc:
Subject: PKI Enabling
Signed By: [redacted]@jtfgno.mil
JTF-GNO Customer Notice

Digitally Signed and Encrypted Message


PKI Enabling
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: JTF-GNO Service Desk Sent: Thu 10/5/2006 5:39 PM
To: JTF-GNO (All Users)
Cc:
Subject: PKI Enabling
Signed By: [redacted]@jtfgno.mil
JTF-GNO Customer Notice

Awareness

Be aware of current information systems threats and targets within DOD

Command and organization Information Security professionals should be following these current threats and continually educating you on them. Specific reports and alerts are published by JTF-GNO.

Resources / Further Details

- **JTF-GNO Portal:**
  NIPRNET: https://www.jtfgno.mil (CAC required)
  JTF-GNO J2/J3 Alert 066-06 (PDF, CAC required)
  SIPRNET: http://www.jtfgno.smil.mil

- **DOD Information Awareness Training**
  http://iase.disa.mil/dodiaa/launchPage.htm

The End

The JTF-GNO directs the operation and defense of the Global Information Grid across strategic, operational, and tactical boundaries in support of DoD's full spectrum of war fighting, intelligence, and business operations.